BEST AVAILABLE COPY

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1.-3. (Cancelled).

4. (Currently amended) A method of email access control, comprising the steps of:

receiving a personalized access ticket containing a sender's identification and a recipient's identification in correspondence and ~~the~~ a sender's identification presented by ~~from~~ a sender from the sender who wishes to send an email to a recipient so as to specify the recipient as an intended destination of the email, the personalized access ticket further containing a validity period indicating a period for which the personalized access ticket is valid, at a secure communication service for connecting communications between the sender and the ~~receiver~~ recipient;

controlling accesses between the sender and the recipient by verifying an access right of the sender with respect to the recipient according to the personalized access ticket at the secure communication service ~~and~~;

checking whether the sender's identification presented by the sender is contained as the sender's identification in the personalized access ticket presented by the sender, and refusing ~~a~~ delivery of the email when the sender's identification presented by the sender is not contained in the personalized access ticket presented by the sender; and

checking the validity period contained in the personalized access ticket presented by the sender, and refusing delivery of the email when the validity period has expired.

5. (Cancelled).

6. (Currently amended) The method of claim ~~5~~ 4, wherein the validity period of the personalized access ticket is set by a trusted third party.

PAGE 6/30 * RCVD AT 2/21/2006 10:07:57 AM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/35 * DNIS:2738300 * CSID:404 815 6555 * DURATION (mm-ss):10-04

BEST AVAILABLE COPY

7. (Previously presented) The method of claim 4, further comprising the step of:

issuing the personalized access ticket to the sender at a directory service for managing an identification of each registrant and a disclosed information of each registrant which has a lower secrecy than a personal information, in a state which is accessible for search by unspecified many, in response to search conditions specified by the sender, by using an identification of a registrant whose disclosed information matches the search conditions as the recipient's identification and the sender's identification specified by the sender along with the search conditions.

8. (Currently amended) The method of claim 4, further comprising the step of:

registering in advance ~~the~~ a personalized access ticket containing an identification of a specific user from which ~~a~~ delivery of emails to a specific registrant is to be refused as ~~the~~ a sender's identification and an identification of the specific registrant as ~~the~~ a recipient's identification for the personalized access ticket registered in advance, at the secure communication service;

wherein at the controlling step the secure communication service refuses ~~a~~ delivery of the email from the sender when the personalized access ticket presented by the sender is registered therein in advance at the registering step.

9. (Original) The method of claim 8, further comprising the step of:

deleting the personalized access ticket registered at the secure communication service upon request from the specific registrant who registered the personalized access ticket at the registering step.

10. (Currently amended) The method of claim 4, wherein the personalized access ticket also contains a transfer control flag indicating whether or not the sender should be authenticated by the secure communication service, and at the controlling step, when the transfer control flag contained in the personalized access ticket indicates that the sender

PAGE 7/30 * RCVD AT 2/21/2006 10:07:57 AM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/35 * DNIS:2738300 * CSID:404 815 6555 * DURATION (mm-ss):10-04

should be authenticated, the secure communication service authenticates the sender's identification presented by the sender and refuses a delivery of the email when an authentication of the sender's identification presented by the sender fails.

11. (Currently amended) The method of claim 10, wherein the authentication of the sender's identification presented by the sender is realized by a challenge/response procedure between the sender and the secure communication service.

12. (Original) The method of claim 10, wherein the transfer control flag of the personalized access ticket is set by a trusted third party.

13. (Previously presented) The method of claim 4, wherein the sender's identification and the recipient's identification in the personalized access ticket are given by real email addresses of the sender and the recipient.

14. (Previously presented) The method of claim 4, wherein the sender's identification and the recipient's identification in the personalized access ticket are given by anonymous identifications of the sender and the recipient, where an anonymous identification of each user contains at least one fragment of an official identification of each user by which each user is uniquely identifiable by a certification authority.

15. (Original) The method of claim 14, wherein the anonymous identification of each user is an information containing the at least one fragment of the official identification of each user which is signed by the certification authority using a secret key of the certification authority.

16. (Original) The method of claim 14, wherein the official identification of each user is a character string uniquely assigned to each user by the certification authority and a public key of each user which are signed by a secret key of the certification authority.

PAGE 8/30 * RCVD AT 2/21/2006 10:07:57 AM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/35 * DNIS:2738300 * CSID:404 815 6555 * DURATION (mm-ss):10-04

17. (Original) The method of claim 14, further comprising the step of:

probabilistically identifying an identity of the sender by reconstructing the official identification of the sender by judging identity of a plurality of anonymous identifications of the sender contained in a plurality of personalized access tickets used by the sender.

18. (Previously presented) The method of claim 4, wherein an anonymous identification of each user that contains at least one fragment of an official identification of each user by which each user is uniquely identifiable by a certification authority and a link information of each anonymous identification by which each anonymous identification can be uniquely identified are defined, and the sender's identification and the recipient's identification in the personalized access ticket are given by a link information of the anonymous identification of the sender and a link information of the anonymous identification of the recipient.

19. (Currently amended) The method of claim 4-18, wherein the link information of each anonymous identification is an identifier uniquely assigned to each anonymous identification by the certification authority.

20. (Original) The method of claim 18, further comprising the step of:

probabilistically identifying an identity of the sender by reconstructing the official identification of the sender by judging identity of a plurality of anonymous identifications of the sender corresponding to the link information contained in a plurality of personalized access tickets used by the sender.

21. (Previously presented) The method of claim 4, wherein the personalized access ticket contains a single sender's identification and a single recipient's identification in 1-to-1 correspondence.

PAGE 9/30 * RCVD AT 2/21/2006 10:07:57 AM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/35 * DNIS:2738300 * CSID:404 815 6555 * DURATION (mm-ss):10-04

22. (Previously presented) The method of claim 4, wherein the personalized access ticket contains a single sender's identification and a plurality of recipient's identifications in 1-to-N correspondence, where N is an integer greater than 1.

23. (Original) The method of claim 22, wherein one identification among the single sender's identification and the plurality of recipient's identifications is a holder identification for identifying a holder of the personalized access ticket while other identifications among the single sender's identification and the plurality of recipient's identifications are member identifications for identifying members of a group to which the holder belongs.

24. (Original) The method of claim 23, further comprising the step of:

issuing an identification of each user and an enabler of the identification of each user indicating a right to change the personalized access ticket containing the identification of each user as the holder identification, to each user at a certification authority, such that prescribed processing on the personalized access ticket can be carried out at a secure processing device only by a user who presented both the holder identification contained in the personalized access ticket and the enabler corresponding to the holder identification to the secure processing device.

25. (Original) The method of claim 24, wherein the certification authority issues the enabler of the identification of each user as an information indicating that it is the enabler and the identification of each user itself which are signed by a secret key of the certification authority.

PAGE 10/30 * RCVD AT 2/21/2006 10:07:57 AM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/35 * DNIS:2738300 * CSID:404 815 6555 * DURATION (mm-ss):10-04

26. (Original) The method of claim 24, wherein the prescribed processing includes a generation of a new personalized access ticket, a merging of a plurality of personalized access tickets, a splitting of one personalized access ticket into a plurality of personalized access tickets, a changing of the holder of the personalized access ticket, changing of a validity period of the personalized access ticket, and a changing of a transfer control flag of the personalized access ticket.

27. (Original) The method of claim 26, wherein a special identification and a special enabler corresponding to the special identification which are known to all users are defined such that the generation of a new personalized access ticket and the changing of the holder of the personalized access ticket can be carried out by the holder of the personalized access ticket by using the special identification and the special enabler without using an enabler of a member identification.

28. (Original) The method of claim 27, wherein the special identification is defined to be capable of being used only as the holder identification of the personalized access ticket.

29. (Original) The method of claim 26, wherein a special identification which is known to all users is defined such that a read only attribute can be set to the personalized access ticket by using the special identification.

30. (Currently amended) The method of claim 4, wherein at the controlling step, when the access right of the sender with respect to the recipient is verified according to the personalized access ticket, the secure communication service takes out the recipient's identification from the personalized access ticket by using the sender's identification presented by the sender, converts the email by using a the taken out recipient's identification into a format that can be interpreted by an email transfer function for actually carrying out a email delivery processing, and gives the email after conversion to the email transfer function by attaching the personalized access ticket.

PAGE 11/30 * RCVD AT 2/21/2006 10:07:57 AM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/35 * DNIS:2738300 * CSID:404 815 6555 * DURATION (mm-ss):10-04

31. (Cancelled).

32. (Currently amended) A method of email access control, comprising the steps of:

defining an official identification of each user by which each user is uniquely identifiable by a certification authority, and an anonymous identification of each user containing at least one fragment of the official identification; ~~and~~

identifying each user by the anonymous identification of each user in communications for emails on a communication network;, wherein the anonymous identification of each user is an information containing the at least one fragment of the official identification of each user which is signed by the certification authority using a secret key of the certification authority;

receiving a personalized access ticket containing a sender's anonymous identification and a recipient's anonymous identification in correspondence, which is presented by a sender who wishes to send an email to a recipient so as to specify the recipient as an intended destination of the email, at a secure communication service for connecting communications between the sender and the receiver; and

controlling accesses between the sender and the recipient by verifying an access right of the sender with respect to the recipient according to the personalized access ticket at the secure communication service.

33. (Previously Presented) The method of claim 32, wherein the official identification of each user is a character string uniquely assigned to each user by the certification authority and a public key of each user which are signed by a secret key of the certification authority.

34. (Cancelled).

PAGE 12/30 * RCVD AT 2/21/2006 10:07:57 AM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/35 * DNIS:2738300 * CSID:404 815 6555 * DURATION (mm-ss):10-04

35. (Currently amended) The method of claim ~~34~~ 32, further comprising the step of:

probabilistically identifying an identity of the sender at the secure communication service by reconstructing the official identification of the sender while judging identity of a plurality of anonymous identifications of the sender contained in a plurality of personalized access tickets used by the sender.

36. (Previously presented) The method of claim 32, wherein the defining step also defines a link information of each anonymous identification by which each anonymous identification can be uniquely identified, and each anonymous identification also contains the link information of each anonymous identification.

37. (Original) The method of claim 36, wherein the link information of each anonymous identification is an identifier uniquely assigned to each anonymous identification by the certification authority.

38. (Currently amended) The method of claim 36, wherein ~~further comprising the steps of:~~

~~receiving a~~ the personalized access ticket contains ~~containing~~ a link information of ~~a~~ the sender's anonymous identification and a link information of ~~a~~ the recipient's anonymous identification ~~in correspondence, which is presented by a sender who wishes to send an email to a recipient so as to specify the recipient as an intended destination of the email, at a secure communication service for connecting communications between the sender and the receiver; and~~

~~controlling accesses between the sender and the recipient by verifying an access right of the sender with respect to the recipient according to the personalized access ticket at the secure communication service~~.

PAGE 13/30 * RCVD AT 2/21/2006 10:07:57 AM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/35 * DNIS:2738300 * CSID:404 815 6555 * DURATION (mm-ss):10-04

39. (Original) The method of claim 38, further comprising the step of:

probabilistically identifying an identity of the sender by reconstructing the official identification of the sender while judging identity of a plurality of anonymous identifications of the sender corresponding to the link information contained in a plurality of personalized access tickets used by the sender.

40.-41. (Cancelled).

42. (Currently amended) A communication system realizing email access control, comprising:

a communication network to which a plurality of user terminals are connected;

a secure communication service device for connecting communications between a sender and a receiver on the communication network, by receiving a personalized access ticket containing a sender's identification and a recipient's identification in correspondence, which is presented by a sender who wishes to send an email to a recipient so as to specify the recipient as an intended destination of the email, the personalized access ticket further containing a validity period indicating a period for which the personalized access ticket is valid, authenticating and controlling accesses between the sender and the recipient by verifying an access right of the sender with respect to the recipient according to the personalized access ticket and by checking the validity period contained in the personalized access ticket presented by the sender, and refusing delivery of the email when the validity period has expired; and

a secure processing device for issuing the personalized access ticket which is signed by a secret key of the secure processing device;

wherein the secure communication service device authenticates the personalized access ticket by verifying a signature of the secure processing device in the personalized access ticket using a public key of the secure processing device.

PAGE 14/30 * RCVD AT 2/21/2006 10:07:57 AM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/35 * DNIS:2738300 * CSID:404 815 6555 * DURATION (mm-ss):10-04

43. (Currently amended) The system of claim ~~40~~ 42, wherein the secure communication service device also receives ~~the~~ a sender's identification presented by the sender along with the personalized access ticket, checks whether the sender's identification presented by the sender is contained in the personalized access ticket presented by the sender, and refuses a delivery of the email when the sender's identification presented by the sender is not contained in the personalized access ticket presented by the sender.

44. (Cancelled).

45. (Currently amended) The system of claim ~~44~~ 42, further comprising:

a trusted third party for setting the validity period of the personalized access ticket.

46. (Currently amended) The system of claim 42, further comprising:

a directory service device for managing an identification of each registrant and ~~and~~ a disclosed information of each registrant which has a lower secrecy than a personal information, in a state which is accessible for search by unspecified many, and issuing the personalized access ticket to the sender in response to search conditions specified by the sender, by using an identification of a registrant whose disclosed information matches the search conditions as the recipient's identification and the sender's identification specified by the sender along with the search conditions.

47. (Currently amended) The system of claim 42, wherein the secure communication service device registers in advance ~~the~~ a personalized access ticket containing an identification of a specific user from which ~~a~~ delivery of emails to a specific registrant is to be refused as ~~the~~ a sender's identification and an identification of the specific registrant as ~~the~~ a recipient's identification of the personalized access ticket registered in advance, and refuses ~~a~~ delivery of the email from the sender when the personalized access ticket presented by the sender is registered therein in advance.

PAGE 15/30 * RCVD AT 2/21/2006 10:07:57 AM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/35 * DNIS:2738300 * CSID:404 815 6555 * DURATION (mm-ss):10-04

48. (Original) The system of claim 47, wherein the secure communication service device deletes the personalized access ticket registered therein upon request from the specific registrant who registered the personalized access ticket.

49. (Currently amended) The system of claim 42, wherein the personalized access ticket also contains a transfer control flag indicating whether or not the sender should be authenticated by the secure communication service, and when the transfer control flag contained in the personalized access ticket indicates that the sender should be authenticated, the secure communication service device authenticates the sender's identification presented by the sender and refuses a delivery of the email when an authentication of the sender's identification presented by the sender fails.

50. (Currently amended) The system of claim 49, wherein the authentication of the sender's identification presented by the sender is realized by a challenge/response procedure between the sender and the secure communication service device.

51. (Original) The system of claim 49, further comprising a trusted third party for setting the transfer control flag of the personalized access ticket.

52. (Previously presented) The system of claim 42, wherein the sender's identification and the recipient's identification in the personalized access ticket are given by real email addresses of the sender and the recipient.

53. (Previously presented) The system of claim 42, further comprising:

a certification authority device for issuing an anonymous identification of each user which contains at least one fragment of an official identification of each user by which each user is uniquely identifiable by the certification authority device;

wherein the sender's identification and the recipient's identification in the personalized access ticket are given by anonymous identifications of the sender and the recipient.

54. (Original) The system of claim 53, wherein the anonymous identification of each user is an information containing the at least one fragment of the official identification of each user which is signed by the certification authority device using a secret key of the certification authority device.

55. (Original) The system of claim 53, wherein the official identification of each user is a character string uniquely assigned to each user by the certification authority device and a public key of each user which are signed by a secret key of the certification authority device.

56. (Original) The system of claim 53, wherein the secure communication service device probabilistically identifies an identity of the sender by reconstructing the official identification of the sender while judging identity of a plurality of anonymous identifications of the sender contained in a plurality of personalized access tickets used by the sender.

57. (Previously presented) The system of claim 42, further comprising:

a certification authority device for issuing an anonymous identification of each user which contains at least one fragment of an official identification of each user by which each user is uniquely identifiable by the certification authority device and a link information of each anonymous identification by which each anonymous identification can be uniquely identified;

wherein the sender's identification and the recipient's identification in the personalized access ticket are given by a link information of the anonymous identification of the sender and a link information of the anonymous identification of the recipient.

58. (Original) The system of claim 57, wherein the link information of each anonymous identification is an identifier uniquely assigned to each anonymous identification by the certification authority device.

PAGE 17/30 * RCVD AT 2/21/2006 10:07:57 AM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/35 * DNIS:2738300 * CSID:404 815 6555 * DURATION (mm-ss):10-04

59. (Original) The system of claim 57, wherein the secure communication service device probabilistically identifies an identity of the sender by reconstructing the official identification of the sender while judging identity of a plurality of anonymous identifications of the sender corresponding to the link information contained in a plurality of personalized access tickets used by the sender.

60. (Previously presented) The system of claim 42, wherein the personalized access ticket contains a single sender's identification and a single recipient's identification in 1-to-1 correspondence.

61. (Previously presented) The system of claim 42, wherein the personalized access ticket contains a single sender's identification and a plurality of recipient's identifications in 1-to-N correspondence, where N is an integer greater than 1.

62. (Original) The system of claim 61, wherein one identification among the single sender's identification and the plurality of recipient's identifications is a holder identification for identifying a holder of the personalized access ticket while other identifications among the single sender's identification and the plurality of recipient's identifications are member identifications for identifying members of a group to which the holder belongs.

63. (Original) The system of claim 62, further comprising:

a certification authority device for issuing to each user an identification of each user and an enabler of the identification of each user indicating a right to change the personalized access ticket containing the identification of each user as the holder identification; and

a secure processing device at which prescribed processing on the personalized access ticket can be carried out only by a user who presented both the holder identification contained in the personalized access ticket and the enabler corresponding to the holder identification to the secure processing device.

PAGE 18/30 * RCVD AT 2/21/2006 10:07:57 AM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/35 * DNIS:2738300 * CSID:404 815 6555 * DURATION (mm-ss):10-04

64. (Original) The system of claim 63, wherein the certification authority device issues the enabler of the identification of each user as an information indicating that it is the enabler and the identification of each user itself which are signed by a secret key of the certification authority device.

65. (Original) The system of claim 63, wherein the prescribed processing includes a generation of a new personalized access ticket, a merging of a plurality of personalized access tickets, a splitting of one personalized access ticket into a plurality of personalized access tickets, a changing of the holder of the personalized access ticket, changing of a validity period of the personalized access ticket, and a changing of a transfer control flag of the personalized access ticket.

66. (Original) The system of claim 65, wherein a special identification and a special enabler corresponding to the special identification which are known to all users are defined such that the generation of a new personalized access ticket and the changing of the holder of the personalized access ticket can be carried out by the holder of the personalized access ticket by using the special identification and the special enabler without using an enabler of a member identification.

67. (Original) The system of claim 66, wherein the special identification is defined to be capable of being used only as the holder identification of the personalized access ticket.

68. (Original) The system of claim 65, wherein a special identification which is known to all users is defined such that a read only attribute can be set to the personalized access ticket by using the special identification.

PAGE 19/30 * RCVD AT 2/21/2006 10:07:57 AM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/35 * DNIS:2738300 * CSID:404 815 6555 * DURATION (mm-ss):10-04

69. (Previously presented) The system of claim 42, wherein when the access right of the sender with respect to the recipient is verified according to the personalized access ticket, the secure communication service device takes out the recipient's identification from the personalized access ticket by using the sender's identification presented by the sender, converts the email by using a the taken out recipient's identification into a format that can be interpreted by an email transfer function for actually carrying out a email delivery processing, and gives the email after conversion to the email transfer function by attaching the personalized access ticket.

70. (Cancelled).

71. (Currently amended) A communication system realizing email access control, comprising:

a certification authority device for defining an official identification of each user by which each user is uniquely identifiable by the certification authority device, and an anonymous identification of each user which contains at least one fragment of the official identification wherein the anonymous identification of each user contains the at least one fragment of the official identification of each user which is signed by the certification authority device using a secret key of the certification authority device; and

an access control device for controlling email accesses to a communication network on which each user is identified by the anonymous identification of each user in communications for emails on the communication network; and

a secure communication service device for connecting communications between users on the communication network by receiving a personalized access ticket containing a sender's anonymous identification and a recipient's anonymous identification in correspondence, which is presented by a sender who wishes to send an email to a recipient so as to specify the recipient as an intended destination of the email, and controlling accesses between the sender and the recipient by verifying an access right of the sender with respect to the recipient according to the personalized access ticket.

PAGE 20/30 * RCVD AT 2/21/2006 10:07:57 AM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/35 * DNIS:2738300 * CSID:404 815 6555 * DURATION (mm-ss):10-04

72. (Previously presented) The system of claim 71, wherein the official identification of each user is a character string uniquely assigned to each user by the certification authority device and a public key of each user which are signed by a secret key of the certification authority device.

73. (Cancelled).

74. (Currently amended) The system of claim ~~73~~ 71, wherein the secure communication service device probabilistically identifies an identity of the sender by reconstructing the official identification of the sender while judging identity of a plurality of anonymous identifications of the sender contained in a plurality of personalized access tickets used by the sender.

75. (Previously presented) The system of claim 71, wherein the certification authority device also defines a link information of each anonymous identification by which each anonymous identification can be uniquely identified, and each anonymous identification also contains the link information of each anonymous identification.

76. (Original) The system of claim 75, wherein the link information of each anonymous identification is an identifier uniquely assigned to each anonymous identification by the certification authority device.

PAGE 21/30 * RCVD AT 2/21/2006 10:07:57 AM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/35 * DNIS:2738300 * CSID:404 815 6555 * DURATION (mm-ss):10-04

77. (Currently amended) The system of claim 75, ~~further comprising: a secure communication service device for connecting communications between the sender and the receiver on the communication network, by receiving a~~ wherein the personalized access ticket contains ~~containing~~ a link information of ~~a~~ the sender's anonymous identification and a link information of ~~a~~ the recipient's anonymous identification in correspondence~~, which is presented by a sender who wishes to send an email to a recipient so as to specify the recipient as an intended destination of the email, and controlling accesses between the sender and the recipient by verifying an access right of the sender with respect to the recipient according to the personalized access ticket~~.

78. (Original) The system of claim 77, wherein the secure communication service device probabilistically identifies an identity of the sender by reconstructing the official identification of the sender while judging identity of a plurality of link informations of anonymous identifications of the sender contained in a plurality of personalized access tickets used by the sender.

79.-81. (Cancelled).

82. (Currently amended) A secure communication service device for use in a communication system realizing email access control, comprising:

computer hardware; and

computer software for causing the computer hardware to connect communications between a sender and a receiver by receiving a personalized access ticket containing a sender's identification and a recipient's identification in correspondence, which is presented by ~~a~~ the sender who wishes to send an email to ~~a~~ the recipient so as to specify the recipient as an intended destination of the email, the personalized access ticket further containing a validity period indicating a period for which the personalized access ticket is valid, and controlling accesses between the sender and the recipient by verifying an access right of the sender with respect to the recipient according to the personalized access ticket;

PAGE 22/30 * RCVD AT 2/21/2006 10:07:57 AM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/35 * DNIS:2738300 * CSID:404 815 6555 * DURATION (mm-ss):10-04

wherein the computer software causes the computer hardware to also receive the sender's identification presented by the sender along with the personalized access ticket, check whether the sender's identification presented by the sender is contained in the personalized access ticket presented by the sender and whether the validity period contained in the personalized access ticket presented by the sender has expired, and refuse a delivery of the email when the sender's identification presented by the sender is not contained in the personalized access ticket presented by the sender or when the validity period has expired.

83. (Cancelled).

84. (Currently amended) The secure communication service device of claim 82, wherein the computer software causes the computer hardware to register in advance ~~the~~ a personalized access ticket containing an identification of a specific user from which a delivery of emails to a specific registrant is to be refused as ~~the~~ a sender's identification and an identification of the specific registrant as ~~the~~ a recipient's identification for the personalized access ticket registered in advance, at the secure communication service device, and refuse ~~a~~ delivery of the email from the sender when the personalized access ticket presented by the sender is registered at the secure communication service device in advance.

85. (Original) The secure communication service device of claim 84, wherein the computer software causes the computer hardware to delete the personalized access ticket registered at the secure communication service device upon request from the specific registrant who registered the personalized access ticket.

86. (Previously presented) The secure communication service device of claim 82, wherein the personalized access ticket also contains a transfer control flag indicating whether or not the sender should be authenticated by the secure communication service device, and when the transfer control flag contained in the personalized access ticket indicates that the sender should be authenticated, the computer software causes the computer hardware to authenticate

PAGE 23/30 * RCVD AT 2/21/2006 10:07:57 AM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/35 * DNIS:2738300 * CSID:404 815 6555 * DURATION (mm-ss):10-04

the sender's identification presented by the sender and refuse a delivery of the email when an authentication of the sender's identification presented by the sender fails.

87. (Currently amended) The secure communication service device of claim 86, wherein the computer software causes the computer hardware to realize the authentication of the sender's identification presented by the sender by a challenge/response procedure between the sender and the secure communication service device.

88. (Previously presented) The secure communication service device of claim 82, wherein the sender's identification and the recipient's identification in the personalized access ticket are given by anonymous identifications of the sender and the recipient, where an anonymous identification of each user contains at least one fragment of an official identification of each user by which each user is uniquely identifiable by a certification authority, and the computer software also causes the computer hardware to probabilistically identify an identity of the sender by reconstructing the official identification of the sender by judging identity of a plurality of anonymous identifications of the sender contained in a plurality of personalized access tickets used by the sender.

89. (Previously presented) The secure communication service device of claim 82, wherein an anonymous identification of each user that contains at least one fragment of an official identification of each user by which each user is uniquely identifiable by a certification authority and a link information of each anonymous identification by which each anonymous identification can be uniquely identified are defined, the sender's identification and the recipient's identification in the personalized access ticket are given by a link information of the anonymous identification of the sender and a link information of the anonymous identification of the recipient, and the computer software also causes the computer hardware to probabilistically identify an identity of the sender by reconstructing the official identification of the sender by judging identity of a plurality of anonymous identifications of

PAGE 24/30 * RCVD AT 2/21/2006 10:07:57 AM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/35 * DNIS:2738300 * CSID:404 815 6555 * DURATION (mm-ss):10-04

the sender corresponding to the link information contained in a plurality of personalized access tickets used by the sender.

90. (Previously presented) The secure communication service device of claim 82, wherein when the access right of the sender with respect to the recipient is verified according to the personalized access ticket, the computer software causes the computer hardware to take out the recipient's identification from the personalized access ticket by using the sender's identification presented by the sender, convert the email by using a the taken out recipient's identification into a format that can be interpreted by an email transfer function for actually carrying out a email delivery processing, and give the email after conversion to the email transfer function by attaching the personalized access ticket.

91.-96. (Cancelled).

97. (Currently amended) A computer usable medium having computer readable program code means embodied therein for causing a computer to function as a secure communication service device for use in a communication system realizing email access control, the computer readable program code means includes:

first computer readable program code means for causing said computer to receive a personalized access ticket containing a sender's identification and a recipient's identification in correspondence, which is presented by a sender who wishes to send an email to a recipient so as to specify the recipient as an intended destination of the email, the personalized access ticket further containing a validity period indicating a period for which the personalized access ticket is valid; and

second computer readable program code means for causing said computer to control accesses between the sender and the recipient by verifying an access right of the sender with respect to the recipient according to the personalized access ticket, so as to connect communications between the sender and the receiver on the communication network;

PAGE 25/30 * RCVD AT 2/21/2006 10:07:57 AM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/35 * DNIS:2738300 * CSID:404 815 6555 * DURATION (mm-ss):10-04

wherein the second computer readable program code means causes said computer to authenticate the personalized access ticket presented by the sender, check whether the validity period contained in the personalized access ticket presented by the sender has expired, and refuse a delivery of the email when the personalized access ticket presented by the sender has been altered or when the validity period has expired.

98. (Original) The computer usable medium of claim 97, wherein the personalized access ticket is signed by a secret key of a secure processing device which issued the personalized access ticket, and the second computer readable program code means causes said computer to authenticate the personalized access ticket by verifying a signature of the secure processing device in the personalized access ticket using a public key of the secure processing device.

99. (Previously presented) The computer usable medium of claim 97, wherein the first computer readable program code means causes said computer to also receive the sender's identification presented by the sender along with the personalized access ticket, and the second computer readable program code means causes said computer to check whether the sender's identification presented by the sender is contained in the personalized access ticket presented by the sender and refuse a delivery of the email when the sender's identification presented by the sender is not contained in the personalized access ticket presented by the sender.

100. (Cancelled).

101. (Previously presented) The computer usable medium of claim 97, wherein the second computer readable program code means causes said computer to register in advance ~~the~~ a personalized access ticket containing an identification of a specific user from which a delivery of emails to a specific registrant is to be refused as the sender's identification and an identification of the specific registrant as the recipient's identification for the personalized

PAGE 26/30 * RCVD AT 2/21/2006 10:07:57 AM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/35 * DNIS:2738300 * CSID:404 815 6555 * DURATION (mm-ss):10-04

access ticket registered in advance, at the secure communication service device, and refuse a delivery of the email from the sender when the personalized access ticket presented by the sender is registered at the secure communication service device in advance.

102. (Original) The computer usable medium of claim 101, wherein the second computer readable program code means causes said computer to delete the personalized access ticket registered at the secure communication service device upon request from the specific registrant who registered the personalized access ticket.

103. (Previously presented) The computer usable medium of claim 97, wherein the personalized access ticket also contains a transfer control flag indicating whether or not the sender should be authenticated by the secure communication service device, and when the transfer control flag contained in the personalized access ticket indicates that the sender should be authenticated, the second computer readable program code means causes said computer to authenticate the sender's identification presented by the sender and refuse a delivery of the email when an authentication of the sender's identification presented by the sender fails.

104. (Currently amended) The computer usable medium of claim 103, wherein the second computer readable program code means causes said computer to realize the authentication of the sender's identification presented by the sender by a challenge/response procedure between the sender and the secure communication service device.

105. (Previously presented) The computer usable medium of claim 97, wherein the sender's identification and the recipient's identification in the personalized access ticket are given by anonymous identifications of the sender and the recipient, where an anonymous identification of each user contains at least one fragment of an official identification of each user by which each user is uniquely identifiable by a certification authority, and the second computer readable program code means also causes said computer to probabilistically

PAGE 27/30 * RCVD AT 2/21/2006 10:07:57 AM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/35 * DNIS:2738300 * CSID:404 815 6555 * DURATION (mm-ss):10-04

identify an identity of the sender by reconstructing the official identification of the sender by judging identity of a plurality of anonymous identifications of the sender contained in a plurality of personalized access tickets used by the sender.

106. (Previously presented) The computer usable medium of claim 97, wherein an anonymous identification of each user that contains at least one fragment of an official identification of each user by which each user is uniquely identifiable by a certification authority and a link information of each anonymous identification by which each anonymous identification can be uniquely identified are defined, the sender's identification and the recipient's identification in the personalized access ticket are given by a link information of the anonymous identification of the sender and a link information of the anonymous identification of the recipient, and the second computer readable program code means also causes said computer to probabilistically identify an identity of the sender by reconstructing the official identification of the sender by judging identity of a plurality of anonymous identifications of the sender corresponding to the link information contained in a plurality of personalized access tickets used by the sender.

107. (Currently amended) The computer usable medium of claim 97, wherein when the access right of the sender with respect to the recipient is verified according to the personalized access ticket, the second computer readable program code means causes said computer to take out the recipient's identification from the personalized access ticket by using the sender's identification presented by the sender, convert the email by using a the taken out recipient's identification into a format that can be interpreted by an email transfer function for actually carrying out a email delivery processing, and give the email after conversion to the email transfer function by attaching the personalized access ticket.

108.-112. (Cancelled).

PAGE 28/30 * RCVD AT 2/21/2006 10:07:57 AM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/35 * DNIS:2738300 * CSID:404 815 6555 * DURATION (mm-ss):10-04

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.